Low-Level Design (LLD): Smart & Secure Campus IT Infra

Project Name	Smart & Secure Campus IT Infra, XYZ Technopark Pune
Project Sponsor	GYANAMGURU
Project Manager	John Alex
Document Type	Low-Level Design
Version	v1.0
Status	Draft

1. Document Purpose

This Low-Level Design template captures the detailed configuration design required to implement VLANs, routing, NAT, firewall policies, wireless networks, and VPN services for the Smart & Secure Campus IT Infra project.

2. Design Inputs and Assumptions

Item	Detail
Site	XYZ Technopark Pune
Internet Service Provider	[ISP name, circuit ID, public IP block]
Firewall Platform	[Vendor / model / HA mode]
Switching Platform	[Core / distribution / access switch models]
Wireless Platform	[WLC / cloud controller / AP model]
VPN Type	[SSL VPN / IPsec remote access / site-to-site VPN]

3. VLAN Design

VLAN ID	VLAN Name	Subnet / Mask	Gateway / SVI	DHCP Scope	Purpose
10	Corporate-LAN	[10.x.x.0/24]	[10.x.x.1]	[Start - End]	Corporate users and endpoints

20	Server	[10.x.x.0/24]	[10.x.x.1]	[Static / Reserved]	Servers and shared services
30	Voice	[10.x.x.0/24]	[10.x.x.1]	[Start - End]	IP phones and voice services
40	Guest-WiFi	[10.x.x.0/24]	[10.x.x.1]	[Start - End]	Guest wireless internet access
50	CCTV	[10.x.x.0/24]	[10.x.x.1]	[Static / Reserved]	IP cameras and NVR systems
60	Access-Control	[10.x.x.0/24]	[10.x.x.1]	[Static / Reserved]	Door controllers and biometric devices
70	Management	[10.x.x.0/24]	[10.x.x.1]	[Restricted]	Network, firewall, wireless, and server management
80	VPN-Users	[10.x.x.0/24]	[Firewall pool]	[VPN pool]	Remote VPN user address pool

4. Switch Port and Trunk Design

Device	Interface	Port Type	Native VLAN	Allowed VLANs	Description
[Core Switch]	[Interface]	Trunk	[VLAN]	[10,20,30,40,50,60,70,80]	Uplink to access switch / firewall / WLC
[Access Switch]	[Interface range]	Access	N/A	[VLAN ID]	User / camera / AP / access-control endpoint ports
[Access Switch]	[Interface]	Trunk	[VLAN]	[Allowed VLAN list]	Uplink to core/distribution switch

5. Routing Design

Route Type	Source Device	Destination / Prefix	Next Hop	Purpose

Default Route	[Core / firewall]	0.0.0.0/0	[Firewall inside / ISP next hop]	Internet-bound traffic
Connected Routes	[Core switch]	[VLAN subnets]	Directly connected	Inter-VLAN routing
Static Route	[Firewall]	[Internal VLAN summary]	[Core switch IP]	Return route to internal networks
VPN Route	[Firewall]	[Remote subnet / VPN pool]	[VPN tunnel / virtual interface]	Remote access or site-to-site connectivity

6. NAT Design

NAT Type	Source	Destination	Translated Address	Interface / Zone	Notes
Dynamic PAT	Internal VLANs	Internet	[Firewall public interface IP]	Inside to Outside	Outbound internet access
Static NAT	[Internal server IP]	Internet	[Public IP]	DMZ / Inside to Outside	Only if publishing internal service
No NAT / NAT Exemption	Internal VLANs	VPN remote subnet / VPN pool	Original source	Inside to VPN	Required for VPN traffic where applicable

7. Firewall Zone and Policy Design

Source Zone	Destination Zone	Service / Port	Action	Logging	Remarks
Corporate LAN	Internet	HTTP/HTTPS/DNS/NTP	Allow	Enable	Standard user internet access
Guest Wi-Fi	Internet	HTTP/HTTPS/DNS	Allow	Enable	Internet-only; block

					internal access
Guest Wi-Fi	Internal Networks	Any	Deny	Enable	Guest isolation
Management	Network Devices	SSH/HTTPS/SNMP/NTP/Syslog	Allow	Enable	Admin-only management access
CCTV	NVR / Security Server	Vendor-specific ports	Allow	Enable	Camera recording and monitoring
Access Control	Access Control Server	Vendor-specific ports	Allow	Enable	Door controller and biometric system connectivity
VPN Users	Approved Internal Services	Required ports only	Allow	Enable	Least-privilege remote access
Any	Any	Any	Deny	Enable	Default cleanup rule

8. Wireless Design

SSID	Mapped VLAN	Authentication	Encryption	User Group	Access Policy
XYZ-Corporate	Corporate-LAN	[802.1X / WPA2-Enterprise / WPA3-Enterprise]	[WPA2/WPA3]	Employees	Internal services and internet as permitted
XYZ-Guest	Guest-WiFi	[Captive portal / PSK]	[WPA2/WPA3]	Visitors	Internet-only; client

					isolation enabled
XYZ-IoT	IoT / Building Systems	[PSK / certificate / MAC auth]	[WPA2/WPA3]	Smart campus devices	Restricted to required services
XYZ-Operations	Management / Operations	[802.1X]	[WPA2/WPA3]	IT and operations team	Privileged access as approved

9. VPN Design

VPN Parameter	Design Value	Remarks
VPN Type	[SSL VPN / IPsec Remote Access / Site-to-Site]	Select based on user and site requirements
Authentication	[Local / AD / LDAP / RADIUS / MFA]	Use strong authentication where available
Address Pool	[VPN user pool]	Must not overlap internal VLANs
Split Tunnel	[Enabled / Disabled]	Define approved internal routes if enabled
Allowed Resources	[Applications / subnets / ports]	Apply least-privilege access
Encryption	[AES-256 / SHA-256 / DH Group]	Align with firewall and security standards
Logging	Enabled	Log authentication, connection, and policy events

10. Validation and Test Plan

Test Area	Test Case	Expected Result	Status
VLAN	Verify endpoint receives correct VLAN and IP address	Endpoint receives correct DHCP/static IP and gateway	[Pass/Fail]

Routing	Verify inter-VLAN routing based on allowed policies	Permitted VLANs communicate; blocked VLANs are denied	[Pass/Fail]
NAT	Verify outbound internet access	Internal clients browse internet using translated public IP	[Pass/Fail]
Firewall	Verify policy allow and deny rules	Approved services are allowed; unauthorized traffic is denied and logged	[Pass/Fail]
Wireless	Verify each SSID maps to correct VLAN	Wireless users receive correct network access and restrictions	[Pass/Fail]
VPN	Verify VPN login and resource access	User authenticates successfully and accesses approved resources only	[Pass/Fail]

11. Approval

Name	Role	Signature	Date
GYANAMGURU	Project Sponsor		
John Alex	Project Manager		
[Name]	Network Architect		
[Name]	Firewall / Security Lead		
[Name]	Wireless Lead		